METHOD AND SYSTEM FOR PROGRAMMING A NON-VOLATILE DEVICE IN A DATA PROCESSING SYSTEM

ABSTRACT

A method and system for insure that code being loaded (flashed) into a flash memory card or other non-volatile storage device of a data processing system is authorized code. The system may include code comprising a kernel portion that transitions the system from a protected-mode to a real-mode and a user portion that includes the code to be loaded onto the flash card. In one embodiment, an asymmetric authentication scheme ensures that the code flashed into the flash card is verified as authorized while complying with the open-source requirements of the operating system. In this embodiment, the public key may become a part of the kernel portion, which is available for all to inspect, while the private key is known only to the user portion. The user portion may generate a signature that is encrypted using the private key. The signature may be generated algorithmically based upon characteristics of or information associated with the corresponding data processing system. The encrypted signature may then be passed as a parameter to the kernel portion, which decrypts the signature according to the public key. If the decrypted signature correctly identifies the system, the kernel potion of the code completes the transition to real-mode and then invokes real-mode flashing code to flash the card. In this manner, only a small portion of code is required to be compiled into the kernel while enabling the code to prevent unauthorized access to the kernel.